

Integral Function Bases

Raymond Hemmecke, Robert Weismantel
Otto-von-Guericke-University Magdeburg

Abstract

Integral bases, a minimal set of solutions to $Ax \leq b, x \in \mathbb{Z}^n$ that generate any other solution to $Ax \leq b, x \in \mathbb{Z}^n$, as a nonnegative integer linear combination, are always finite and are at the core of the Integral Basis Method introduced by Haus, Köppe and Weismantel.

In this paper we present one generalization of the notion of integral bases to the nonlinear situation with the intention of creating an integral basis method also for nonlinear integer programming.

1 Introduction

In the past fifty years many efforts have been undertaken to study linear integer optimization problems from different mathematical and algorithmic viewpoints. As a result, a basic understanding of the geometry of integer programming problems defined by linear equations and/or linear inequalities is present today. This knowledge has been partly turned into algorithmic tools to tackle discrete optimization problems in practice.

The attempts to study the geometry of integer points in polyhedral sets are based on two basic mathematical concepts. One is the notion of a lattice. More precisely, a basis of a lattice L is a subset of linearly independent vectors that allows one to generate all points in the lattice with respect to taking integer linear combinations. The geometric properties of particular bases in lattices made it possible to design algorithms for solving specific linear integer programming problems, mainly problems without lower and upper bounds on the variables and linear problems with a fixed number of discrete variables [5, 6]. The notion of bases of a lattice can be further refined so as to yield so-called integral generating sets for cones and polyhedra. Roughly speaking, integral generating sets extend – besides lattices – the notions of extreme points and rays in polyhedra and cones to integer points in such sets. More precisely, an integral generating set for a set $S \subseteq \mathbb{Z}^n$ is a subset of S with the property that every member of S can be represented as a nonnegative integer combination of the elements in S . Of course, S itself constitutes an integral generating set of itself. The key question is to detect an integral generating set that is finite and minimal with respect to inclusion. This immediately raises the question to characterize those sets S of lattice points that possess a finite integral generating set. This question is answered in Section 2 of this paper.

Indeed, integral generating sets have important implications for the theory of linear integer programming. Most importantly, optimality conditions for integer optimization problems can be derived through integral generating sets. Such sets also provide a basic understanding of integral polyhedra and totally dual integral systems of inequalities [2]. Last but not least they play a central role in the development of integer simplex type methods of linear integer programs [4]. In fact,

it is quite obvious to see that if a finite integral generating set for a discrete set of points is available, then we can reformulate the problem of detecting a particular element in S as the problem of detecting a nonnegative integer multiplier associated with the new representation through an integral generating set. Integral generating sets therefore allow a new representation of the same set S in some other space. The beautiful fact is that if we start off with a set S that is the feasible region of an integer linear program in nonnegative variables, then also after reformulation the new optimization problem happens to be a linear integer program in nonnegative variables. This follows simply from the fact that the integral generating set enables us to express every point as a nonnegative integer combination.

Suppose now that S does not have a finite integral generating set. This in fact may happen even though S corresponds to all the integer points in a polyhedron. In particular, if the constraints defining S are not linear, even in quite restrictive cases S does not possess a finite integral generating set.

Then the idea to use integral generating sets for reformulation issues is not possible, because the generating set is infinite. We can simply not write down any finite representation of the reformulated problem. In order to cope with this scenario, it requires to generalize the notion of an integral generating set from the linear case to a nonlinear setting. We will refer to such sets as integral function bases, since they enable us to derive representations by means of nonnegative polynomial combinations instead of nonnegative linear combinations. This is the central topic of Section 3. In turn, our generalization allows us to formulate optimality conditions for integer polynomial programming problems.

We also analyze the situation when an integral function basis for the integer points in a complicated semi-algebraic set is replaced by the condition of being members of a relaxation of the semi-algebraic set itself. This question is in particular motivated by the design of pivoting type methods for polynomial integer and mixed integer programming, a topic that we regard as theoretically and practically challenging, but important.

2 Integral Bases

Let us start by defining the notion of an integral basis.

Definition 2.1 *Let $S \subseteq \mathbb{Z}^n$. Then we call $T \subseteq S$ an **integral basis** of S , if for every $s \in S$ there exists a finite (integer) linear combination $s = \sum \alpha_i t_i$ with $t_i \in T$ and $\alpha_i \in \mathbb{Z}_+$.*

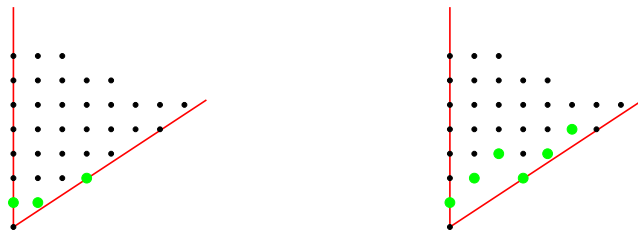


Figure 1: Minimal integral bases of two sets of lattice points

Note that an integral basis of S is allowed to contain elements only from S itself! With this definition, Bertsimas and Weismantel [1] showed the following characterization of which rational polyhedra (or more precisely the integer points in such polyhedra) have a *finite* integral basis.

Theorem 2.2 (Bertsimas and Weismantel [1]) *For $A \in \mathbb{Z}^{d \times n}$ and $b \in \mathbb{Z}^d$, define the sets $P = \{x \in \mathbb{R}_+^n : Ax \leq b\}$, $S = P \cap \mathbb{Z}^n$, and $C = \{x \in \mathbb{R}_+^n : Ax \leq 0\}$.*

- (a) *There exists a finite integral generating set of S if and only if S contains all but finitely many integer points in $C \cap \mathbb{Z}_+^n$.*
- (b) *If a finite integral generating set of S exists, then there is a unique integral basis of S .*

Note that for $b = 0$, this theorem simply states existence (and uniqueness) of a Hilbert basis for the (pointed) rational polyhedral cone $\{x \in \mathbb{R}_+^n : Ax \leq 0\}$.

Now let us give a novel and more general characterization of which sets of lattice points have a finite integral basis. As we do not make any structural assumption on the set of lattice points, we have to be cautious to check whether the integral bases that we construct do indeed consist of lattice points from our original sets only.

Theorem 2.3 *Let $S \subseteq \mathbb{Z}^n$ be any set of lattice points in \mathbb{Z}^n .*

- (a) *S has a finite integral basis if and only if $C = \text{cone}(S)$ is a rational polyhedral cone.*
- (b) *If the cone $C = \text{cone}(S)$ is rational and pointed, there is a unique finite integral basis that is minimal with respect to set inclusion.*

Proof. Let us start showing part (a). If $C = \text{cone}(S)$ is not a rational polyhedral cone, S cannot have a finite integral basis $G \subseteq S$, since $C = \text{cone}(S) = \text{cone}(G)$ would be a rational cone, contradicting our initial assumption on C .

Now we show the remaining claim that S has a finite integral basis if $C = \text{cone}(S)$ is rational by explicitly constructing such a finite basis. It should be noted that this integral basis need not be minimal.

First, let us triangulate C into (finitely many!) simplicial cones C_1, \dots, C_k . Note that we can and do choose such a triangulation for which the generators of the cones C_i are also among the (finitely many) generators of C . Thus, as C , each cone C_i is generated by (finitely many) elements S_i of S . It remains to show that for each rational simplicial cone $C_i = \text{cone}(S_i)$, the set $C_i \cap S$ has a finite integral basis G_i . Then the union of all G_i , $i = 1, \dots, k$, is clearly a finite integral basis for S .

For $C_i = \text{cone}(S_i)$ and $S_i = \{v_1, \dots, v_r\}$, consider the parallelepiped

$$F = \left\{ \sum_{j=1}^r \alpha_j v_j : 0 \leq \alpha_1, \dots, \alpha_r < 1 \right\}.$$

As F_i is bounded, F contains only finitely many lattice points $\{f_1, \dots, f_t\}$ in \mathbb{Z}^n . Moreover, $C_i \cap \mathbb{Z}^n$ is the disjoint union of the following t sets F_1, \dots, F_t with

$$F_j = \left\{ f_j + \sum_{j=1}^r \alpha_j v_j : \alpha_1, \dots, \alpha_r \in \mathbb{Z}_+ \right\}.$$

We construct now a finite integral basis for $C_i \cap S$.

Consider any F_j , $j = 1, \dots, t$. As C_i is a simplicial cone, each point in F_j has a unique representation as $f_j + \sum_{j=1}^r \alpha_j v_j$ implying that there is a one-to-one correspondences ϕ_j between F_j and \mathbb{Z}_+^r given by

$$\phi_j \left(f_j + \sum_{j=1}^r \alpha_j v_j \right) = (\alpha_1, \dots, \alpha_r).$$

To construct a finite integral basis for $F_j \cap S$, consider the set $\phi_j(F_j \cap S) \subseteq \mathbb{Z}_+^r$. By the Gordan-Dickson Lemma, there are only finitely many points $\{g_1, \dots, g_p\}$ that are minimal with respect to the partial ordering \leq defined on \mathbb{Z}_+^r . Thus, each point $\phi_j(F_j \cap S)$ can be written as a positive integer linear combination of g_1, \dots, g_p and of the unit vectors e_1, \dots, e_r . Thus, every element in $F_j \cap S$ is a positive integer linear combination of $\phi^{-1}(g_1), \dots, \phi^{-1}(g_p) \in F_j \cap S$ together with $\phi^{-1}(e_1), \dots, \phi^{-1}(e_r) \in S_i \subseteq S$. Let $G_{i,j}$ denote the set of all these vectors. Clearly, the union G_i over all $G_{i,j}$, $j = 1, \dots, t$, forms a finite integral basis for $C_i \cap S$, and claim (a) is proved.

Let us prove claim (b) now. As $\text{cone}(S)$ is pointed, there is some vector $c \in \mathbb{R}^n$ such that $\{x \in \mathbb{R}^n : c^\top x \leq 0\} \cap \text{cone}(S) = \{0\}$. Assume that $U = \{u_1, \dots, u_r\}$ and $V = \{v_1, \dots, v_t\}$ are two different inclusion minimal integral bases of S . Moreover, assume that w.l.o.g. $u_1 \notin V$. Minimality of U implies that u_1 cannot be written as a positive integer linear combination of elements in $U \setminus \{u_1\}$. However, as V is an integral basis of S and $u_1 \in S$, there is a nonnegative integer linear combination $u_1 = \sum_{j=1}^t \alpha_j v_j$. Clearly, as $u_1 \notin V$ and as the coefficients are nonnegative integers, we have $c^\top v_j < c^\top u_1$ whenever $\alpha_j > 0$. As also U is an integral basis of S and as all $v_j \in S$, there are nonnegative integer linear combinations $v_j = \sum_{i=1}^r \beta_{i,j} u_i$. Moreover, $c^\top u_i \leq c^\top v_j$ whenever $\beta_{i,j} > 0$. Plugging these representations into $u_1 = \sum_{j=1}^t \alpha_j v_j$, we get a representation of u_1 as a nonnegative integer linear combination of elements in U . However, by construction, they all have a scalar product with c that is strictly less than $c^\top u_1$. Thus, we have written u_1 as a nonnegative integer linear combination of elements in $U \setminus \{u_1\}$, a contradiction to our assumption that U is a set inclusion minimal integral basis, and the claim is proved. \square

Note that for sets of the form $\{x \in \mathbb{Z}^n : Ax \leq 0\}$, Theorem 2.3 again simply states existence of finite Hilbert bases for rational polyhedral cones and uniqueness of the minimal Hilbert basis if the cone is pointed. It is easy to show that the minimal Hilbert basis of a cone must consist of lattice points from the fundamental parallelepiped and is thus finite. The tricky part for the proof of Theorem 2.3 was the fact, that not all points of this parallelepiped could be assumed to belong to S . The two examples in Figure 1, page 2 already illustrate this difficulty.

Let us now show how Theorem 2.3 implies the special case, Theorem 2.2.

Proof of Theorem 2.2. Let us show part (a) first. If S is finite, nothing is left to show. Thus, assume that S is not finite and therefore also $C \neq \{0\}$. Assume that S contains all but finitely many integer points in $C \cap \mathbb{Z}_+^n$. In particular, S contains an (integer) point of every extreme ray of C . By Minkowski's theorem, we have $\text{conv}(P \cap \mathbb{Z}^n) = \text{conv}(G) + C$, where $G \subseteq S$ is the set of extreme points in $\text{conv}(P \cap \mathbb{Z}^n) \subseteq P$. (Since P does not contain a line, $G \neq \emptyset$.) Thus, $\text{cone}(S) = \text{conv}(G) + C$, as $G \subseteq S$ and as S contains an (integer) point of every extreme ray of C . Consequently, $\text{cone}(S)$ is a rational cone and thus has a finite integral basis by Theorem 2.3.

Now assume that there are infinitely many integer points in C that do not belong to S . In particular, $0 \notin P$ as otherwise $0 = A0 \leq b$ implying $C \subseteq P$ and thus $C \cap \mathbb{Z}^n \subseteq S$. Assume for the moment that each extreme ray of C contains a (nonzero!) point of P . Fix any extreme ray of C and let

$v \in C \cap P$ be a point on this ray. Then any point $w = kv$, $k \geq 1$, on this ray must belong to P . This follows from $Aw = k(Av) = (k-1)v + v \leq (k-1) \cdot 0 + b = b$ and $Av \leq 0$, $Av \leq b$, and $k \geq 1$. Therefore, $w \in P$ as claimed. By convexity of P , P must contain the convex hull H of all these half-lines $\{kv : k \geq 1, k \in \mathbb{R}\}$. As $C \setminus H$ is bounded, only a finite number of integer points in C can lie in $C \setminus H$. As $S = P \cap \mathbb{Z}^n$, this implies that only finitely many integer points C can lie outside of S , contradicting our initial assumption on C . This implies that there must be an extreme ray R of C that does not contain any point of P .

We now show that $\text{cone}(S)$ cannot be a rational cone, and the result follows again by Theorem 2.3. Assume on the contrary that $\text{cone}(S)$ is a rational cone. By convexity of S , every ray in $\text{cone}(S)$ has a nontrivial intersection with S and thus also with P . This implies that the extreme ray R does not belong to $\text{cone}(S)$. As $\text{cone}(S)$ is rational, there exists a finite (rational) description

$$\text{cone}(S) = \{x \in \mathbb{R}^n : c_i^\top x \leq 0, i = 1, \dots, p\}.$$

Let v be any rational vector with $R = \text{cone}(v)$. Then $v \notin \text{cone}(S)$ implies that there is some index j such that $c_j^\top v > 0$. Now consider any integer point $w \in S$. As $S = \text{conv}(G) + C$, all integer points on the half-line $\{w + \alpha v : \alpha \geq 0\}$ belong to S . Moreover, as v is a rational vector, there are infinitely many integer points on this half-line. However, as $c_j^\top v > 0$, we have $c_j^\top (w + \alpha v) > 0$ for sufficiently large α , implying that there are integer points of S that lie outside of $\text{cone}(S)$. This contradiction shows that $\text{cone}(S)$ is not a rational cone and part (a) is proved.

As part (b) of our claim follows now immediately from part (b) of Theorem 2.3, nothing is left to show. \square

A natural question that we may ask is, whether there are other special cases of interesting sets of lattice points that have a finite integral basis by Theorem 2.3.

One natural guess would be the integral points in a convex region. However, convexity alone is not enough to ensure that $\text{cone}(S)$ is rational, as can be seen by looking at a polyhedral cone with irrational generators. Thus, some notion of “rational generators” of the region should be defined.

With this in mind, we may try to look at sets that are parametrized by convex polynomials that have rational coefficients only. Again, there is a simple counter-example. For the lattice points S in the parametrized set

$$\left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 : \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} s \\ s^2 \end{pmatrix} + \begin{pmatrix} 0 \\ t \end{pmatrix}, s, t \in \mathbb{R}_+ \right\},$$

we easily see that $\text{cone}(S)$ is not rational, see Figure 2.

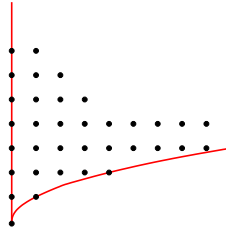


Figure 2: $\text{cone}(S)$ is not rational.

We conclude that even convexity **and** rationality of generators is generally not enough to ensure finiteness of an integral basis. It can be shown that under the assumption that if in addition the given set itself is convex and that if it contains the unit vectors of the positive orthant, a finite integral basis does exist.

3 Nonlinear Integral Bases. Definition and Motivation

Theorem 2.3 characterizes when linear integral bases exist. What can we do if the conditions of the theorem do not hold? For instance, if we consider the set $S = \{(x, y) \in \mathbb{Z}_+^2 : y \geq 1\}$.

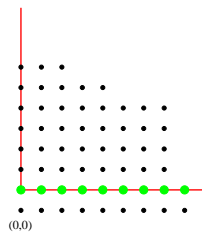


Figure 3: Example of an infinite integral basis

In this case, the set $\text{cone}(S)$ is not finitely generated, and thus there does not exist a finite integral basis of S . For obtaining a finite representation in this example, it becomes necessary to extend the notion of an integral basis to – what we call – an integral function basis. Our goal then becomes to identify sets of points that have a finite integral function basis. In the following we consider sets $S = \{y \in \mathbb{R}^n : y = g(\lambda), \lambda \in \mathbb{Z}_+^d\} \cap \mathbb{Z}^n$, where $g : \mathbb{R}^d \rightarrow \mathbb{R}^n$ is a vector of functions with components $g_i : \mathbb{R}^d \rightarrow \mathbb{R}$, $i = 1, \dots, n$, and with $g(\mathbb{Z}^d) \subseteq \mathbb{Z}^n$.

Note that when all g_i are linear functions, our set S corresponds to the lattice points of a rational polyhedral cone. Other possible functions are polynomials in $\mathbb{Z}[\lambda]$, certain stair-case functions, or even suitable combinations of all 3 types.

Example 3.1 *The function g given by*

$$g = \begin{pmatrix} \lambda_1^2 \\ \lambda_1 + \lambda_2 \end{pmatrix}$$

defines a semi-algebraic set $\mathcal{C} = \{y \in \mathbb{R}^2 : y = g(\lambda), \lambda \in \mathbb{Z}_+^2\}$, see Figure 4. In Cartesian coordinates, \mathcal{C} can be described by $\mathcal{C} = \{(x, y) \in \mathbb{R}^2 : x - y^2 \geq 0, x, y \geq 0\}$.

Of special interest to us will be the lattice points inside semi-algebraic sets.

Definition 3.2 *Consider a set $S \subseteq \mathbb{Z}^n$. Let sets $T_i \subseteq \mathbb{Z}^n$ be given where each T_i is described in the form $T_i := \{f_i(t_i) : t_i \in \mathbb{Z}_+^{n_i}\}$ with a polynomial function $f_i : \mathbb{Z}_+^{n_i} \rightarrow \mathbb{Z}^n$.*

*Then we call such a family $\{T_i\}$ an **integral function basis** of S , if for every $s \in S$ there exists a finite representation, $s = \sum f_i(t_i)$, with $t_i \in \mathbb{Z}_+^{n_i}$ and $f_i(t_i) \in S$.*

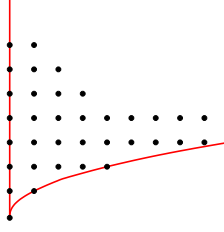


Figure 4: Semi-algebraic set C with its lattice points

If we allowed only linear functions f_i and if S are the lattice points in a rational polyhedral cone, this definition coincides with the definition of a Hilbert basis.

If we reconsider the example with $S = \{(x, y) \in \mathbb{Z}_+^2 : y \geq 1\}$, we see that the following set T_1 defines an integral function basis of S :

$$T_1 = \{f(\lambda, \mu) = (\lambda, 1 + \mu) : \lambda, \mu \in \mathbb{Z}_+\}.$$

Example 3.1, cont. Let us consider again the semi-algebraic set $C = \{(x, y) \in \mathbb{R}^2 : x - y^2 \leq 0, x, y \geq 0\}$. An integral function basis of $S = C \cap \mathbb{Z}^2$ is given by $\{T_1, T_2\}$ with $T_1 = \{(0, t) : t \in \mathbb{Z}_+\}$ and $T_2 = \{((x+1)^2 - s, x+1) : x, s \in \mathbb{Z}_+\}$, where the parameters x and s need to satisfy $s \leq (x+1)^2$ to guarantee $((x+1)^2 - s, x+1) \in S$, see Figure 5. The only lattice point in C that cannot be written as a sum of a lattice point in T_1 and a lattice point in T_2 is the origin. This special point, however, can already be represented by T_1 alone.

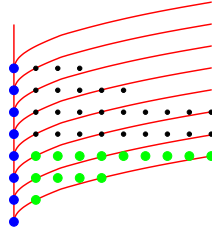


Figure 5: Integral function basis of a semi-algebraic set

Note that the constraints that are needed to encode the condition $(x+1)^2 - s, x+1 \in S$ have the same maximal degree as the original constraints. On the other hand, we can also this condition by $s \leq 2x+1$, see Figure 6. The latter representation should be preferred, since this description of the set S using the integral function basis involves only linear constraints in contrast to the quadratic constraint in the description above. \square

In the following, we outline a fundamental application of integral function bases for nonlinear integer optimization problems. It turns out that one can derive an optimality criterion for a linear integer program with a polynomial objective function. This criterion is a natural generalization of what Graver proved in the fully linear (integer) setting [3].

Theorem 3.3 *Let $p(z)$ be any polynomial in $\mathbb{Z}[z_1, \dots, z_n]$, and let $A \in \mathbb{Z}^{d \times n}$ and $b \in \mathbb{Z}^d$. Consider*

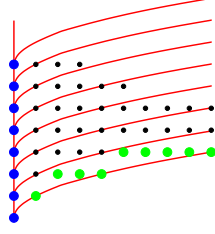


Figure 6: Integral function basis of a semi-algebraic cone

the (possibly nonlinear) integer optimization problem

$$\max\{p(z) : Az = b, z \geq 0, z \in \mathbb{Z}^n\}.$$

Let $W^i \in \mathbb{Z}^{n \times w_i}$, $i = 1, \dots, 2^n$, denote the extreme rays of the cones

$$\text{cone}(W^i) = \{x \in \mathbb{R}^n \cap \mathbb{O}_i : Ax = 0\},$$

where $\mathbb{O}_1, \dots, \mathbb{O}_{2^n}$ denote the 2^n orthants of \mathbb{R}^n . Thus, every point in this cone can be written as a linear combination $z = W^i \lambda$, $\lambda_i \geq 0$.

Assume that z_0 is a feasible integer solution to $Az = b$, $z \geq 0$. For each $i = 1, \dots, 2^n$, define the following vector of nonlinear functions,

$$g^i(\lambda) = \begin{pmatrix} g_1^i(\lambda) \\ \vdots \\ g_n^i(\lambda) \\ \bar{q}^i(\lambda) \end{pmatrix} = \begin{pmatrix} W^i \lambda \\ p(z_0 + W^i \lambda) - p(z_0) \end{pmatrix}.$$

Let $\{T_1^i, \dots, T_{k_i}^i\}$, with $T_j^i := \{f_j^i(t_j) : t_j \in \mathbb{R}_+^{n_{i,j}}\}$, be an integral function basis for the (integer points in the) semi-algebraic set $\mathcal{C}^i = \{y \in \mathbb{R}^{n+1} : y = g^i(\lambda), \lambda \geq 0\}$. Define by $S_{i,j}$ the semi-algebraic set that encodes the conditions $[f_j^i(t_j)]_{1,\dots,n} \in \text{cone}(W^i)$. (Herein, $[f_j^i(t_j)]_{1,\dots,n}$ shall denote the vector of the first n components of $f_j^i(t_j)$.)

Then z_0 is optimal if and only if for every $i = 1, \dots, 2^n$, the following condition holds:

$$[f_j^i(t_j)]_{n+1} \leq 0 \text{ for all } t_j \in \mathbb{Z}_+^{n_{i,j}} \cap S_{i,j} \text{ with } [f_j^i(t_j)]_k \geq -[z_0]_k, \text{ for all } k = 1, \dots, n.$$

Proof. Assume that there is a better feasible solution z_1 that has an objective value $p(z_1) > p(z_0)$. Consider the difference vector $v := z_1 - z_0$, which lies in one of the 2^n orthants \mathbb{O}_i of \mathbb{R}^n . Therefore, we are looking for $v \in \mathbb{O}_i$ with $Av = 0$, $z_0 + v \geq 0$, and $p(z_0 + v) - p(z_0) > 0$. Clearly, the set $\{z \in \mathbb{O}_i : Az = 0\}$ forms a pointed rational cone, generated by the columns of W^i . Thus, $v = W^i \lambda$ for some $\lambda \in \mathbb{R}_+^{w_i}$ and hence

$$\begin{pmatrix} W^i \lambda \\ p(z_0 + W^i \lambda) - p(z_0) \end{pmatrix}$$

is an integer point in the semi-algebraic set $\mathcal{C}^i = \{y \in \mathbb{R}^{n+1} : y = g^i(\lambda), \lambda \geq 0\}$. Using the integral function basis of this set, there is a representation

$$\begin{pmatrix} W^i \lambda \\ p(z_0 + W^i \lambda) - p(z_0) \end{pmatrix} = \sum_{j \in I^i} f_j^i(t_j) = \sum_{j \in I^i} \begin{pmatrix} [f_j^i(t_j)]_{1,\dots,n} \\ [f_j^i(t_j)]_{n+1} \end{pmatrix}$$

with $t_j^i \in S_{i,j} \cap \mathbb{Z}^{n_{i,j}}$ and $f_j^i(t_j) \in \mathcal{C}^i$.

As $p(z_0 + W^i \lambda) - p(z_0) > 0$, there must be some $j \in I^i$ with $[f_j^i(t_j)]_{n+1} > 0$. We claim that the first n components of $f_j^i(t_j) \in \mathcal{C}^i$ form an improving integer vector for z_0 , possibly different from the vector v that we decomposed.

As $[f_j^i(t_j)]_{n+1} > 0$, the only thing left to show is that the components $[f_j^i(t_j)]_1, \dots, [f_j^i(t_j)]_n$ of $f_j^i(t_j)$ lie above the lower bounds, i.e., $[f_j^i(t_j)]_k \geq -[z_0]_k$ for $k = 1, \dots, n$. But this can be seen as follows. By construction, $\text{cone}(W^i) \in \mathbb{O}^i$, implying $[f_j^i(t_j)]_{1,\dots,n} \in \mathbb{O}^i$ for all j . Thus, the components of $z_0 + [f_j^i(t_j)]_{1,\dots,n}$ lie between the components of z_0 and of $z_0 + v = z_1$, and are therefore nonnegative.

The converse direction is obviously true. \square

Clearly, one would wish that searching for an improving vector in each of the T_i is simpler than searching for an improving vector in \mathcal{C} .

The set $T_1 = \{\lambda - \mu : \lambda, \mu \in \mathbb{Z}_+^n\}$ always forms an integral function basis for any set $S \subseteq \mathbb{Z}^n$, where $2n$ parameters are needed to describe T_1 . The following theorem bounds the number of parameters needed in the T_i and thus gives a sufficient condition (together with a construction) of when an integral function basis with less parameters in the description of each T_i exists.

Theorem 3.4 *Let $S \subseteq \mathbb{Z}^n$, $v_1, \dots, v_k \in \mathbb{Z}^n$ and let $C = \text{cone}(v_1, \dots, v_k)$ be a rational polyhedral cone with $S \subseteq C$. Then S has an integral function basis in which the appearing sets T_i involve at most $k + 1$ parameters.*

Proof. First observe that $S \subseteq C$ implies $\text{cone}(S) \subseteq C$ and therefore $\text{cone}(S \cup \{v_1, \dots, v_k\}) = C$. Thus, by Theorem 2.3, there is a finite integral basis $\{h_1, \dots, h_s, v_1, \dots, v_k\}$ for the set $S \cup \{v_1, \dots, v_k\}$. If we set in addition $h_0 = 0$, we can see from the proof of Theorem 2.3, that every point $v \in S$ can be written as $v = h_i + \sum_{j=1}^k \lambda_{ij} v_j$ for some $i \in \{0, \dots, s\}$ and for some nonnegative integers λ_{ij} . This last condition in fact states that the sets $T_i = \{h_i + \sum_{j=1}^k \lambda_{ij} v_j : \lambda_i \in \mathbb{Z}_+^k\} \cup \{0\}$, $i = 0, 1, \dots, s$, form an integral function basis for S . \square

Remark 3.5 *It should be noted that we may strengthen the above theorem if some or all of the cone generators v_j lie in S . If $v_{j_0} \in S$, then each set $T_i = \{h_i + \sum_{j=1}^k \lambda_{ij} v_j : \lambda_i \in \mathbb{Z}_+^k\} \cup \{0\}$ can in fact be decomposed into the sum of $T'_i = \{h_i + \sum_{j \in \{1, \dots, k\} \setminus \{j_0\}} \lambda_{ij} v_j : \lambda_i \in \mathbb{Z}_+^{k-1}\} \cup \{0\}$ and $T''_i = \{\lambda_{ij_0} v_{j_0} : \lambda_{ij_0} \in \mathbb{Z}_+\}$.*

Iterating this process for all cone generators v_j that lie in S gives a new integral function basis for S with fewer parameters appearing in the description of the sets T_i . In fact, if all v_j lie in S , that is if $C = \text{cone}(S)$, the integral function basis for S simplifies to sets T_i that all contain nonnegative integer multiples of a single lattice point of S . Thus, we have recovered the statement of Theorem 2.3: the existence of a finite integral basis if $\text{cone}(S)$ is rational.

The following example demonstrates that splitting the set S into finitely many subsets may also decrease the maximum number of parameters needed in the description of the T_i 's.

Example 3.6 *Consider the set $S = \{(x, y) \in \mathbb{Z}^2 : -y^2 \leq x \leq y^2\}$. As this set is contained in the rational cone spanned by e_1 and $-e_1$, we conclude by Theorem 3.4 that S has an integral function basis, in which each T_i is described by at most $2 + 1 = 3$ parameters.*

However, if we split the set S as

$$S = S' + S'' = \{(x, y) \in \mathbb{Z}^2 : -y^2 \leq x \leq 0\} \cup \{(x, y) \in \mathbb{Z}^2 : 0 \leq x \leq y^2\},$$

we see that $S' \subseteq \text{cone}(-e_1, e_2)$ and $S'' \subseteq \text{cone}(e_1, e_2)$. Since the cone generator e_2 is an element of the sets S' and S'' , respectively, we find integral function bases for S' and S'' , in which each T_i is described by at most $1 + 1 = 2$ parameters. Putting both together, we arrive at an integral function basis for S with the same property. \square

As we have seen above, every set of lattice points in \mathbb{Z}^n admits a representation via an integral function basis. Even under the assumption that we have found a nice integral function basis for a particular problem instance, that is, one that has only few parameters in the description of the T_i , we are faced with a new problem to be solved.

Suppose we want to maximize a (polynomial) function $p(x)$ over the lattice points in a semi-algebraic set \mathcal{C} . Knowing an integral function basis $\{T_i : i \in I\}$, we can use the representation $x = \sum_{i \in I} f_i(t_i)$, $t_i \in \mathbb{Z}^{n_i}$ for all $x \in \mathcal{C} \cap \mathbb{Z}^n$ to rewrite the problem as

$$\max \left\{ p \left(\sum_{i \in I} f_i(t_i) \right) : \sum_{i \in I} f_i(t_i) \in \mathcal{C} \cap \mathbb{Z}^n, t_i \in \mathbb{Z}_+^{n_i} \right\}.$$

While the condition $\sum_{i \in I} f_i(t_i) \in \mathcal{C} \cap \mathbb{Z}^n$ often follows immediately from $f_i(t_i) \in \mathcal{C} \cap \mathbb{Z}^n$ for all $i \in I$, these latter conditions involve descriptions by polynomials of the same degree as in the description of \mathcal{C} and are thus still hard to deal with. Finding $t_i \in \mathbb{Z}_+^{n_i}$ with $f_i(t_i) \in \mathcal{C} \cap \mathbb{Z}^n$ even only for a single i (as needed in Theorem 3.3) is as hard as finding a point in \mathcal{C} , at least from a complexity point of view.

Thus, an integral function basis with the additional property that $T_i \subseteq \mathcal{C} \cap \mathbb{Z}^n$ for all $i \in I$ would be desirable. Then $f_i(t_i) \in \mathcal{C} \cap \mathbb{Z}^n$ for all $i \in I$ and for all $t_i \in \mathbb{Z}^{n_i}$ would hold automatically. For this, of course, a nonlinear description for the T_i is needed, in contrast to the rather nice and simple description guaranteed to exist by Theorem 3.4.

In the following, we relax the condition $f_i(t_i) \in \mathcal{C} \cap \mathbb{Z}^n$ and allow a *correction term* that may lie outside, but which is bounded by polynomials of strictly smaller degree than the given polynomials.

Theorem 3.7 *For every semi-algebraic set*

$$\mathcal{C} := \{x \in \mathbb{R}^n : \exists y \geq 0 \text{ with } x = g(y)\}, g : \mathbb{R}^d \rightarrow \mathbb{R}^n,$$

there exists a set of functions

$$\{g_l, g_u : \mathbb{R}^n \rightarrow \mathbb{R}^n\}$$

with $\maxdeg(g_l), \maxdeg(g_u) < \maxdeg(g)$ and such that for every point $x \in \mathcal{C} \cap \mathbb{Z}^n$ there exists a $\lambda \in \mathbb{Z}_+^d$ and a point $v_x \in \mathbb{Z}^n$ with $x = g(\lambda) + v_x$ and with $g_l(\lambda) \leq v_x \leq g_u(\lambda)$.

Proof. Choose any $x \in S := \mathcal{C} \cap \mathbb{Z}^n$. Then $x = g(y)$ for some $y \in \mathbb{R}_+^d$. Now define $\lambda := \lfloor y \rfloor$ component-wise and let $v_x = x - g(\lambda)$ and $h = y - \lambda$. We will now construct functions $g_l : \mathbb{R}^n \rightarrow \mathbb{R}^n$ and $g_u : \mathbb{R}^n \rightarrow \mathbb{R}^n$, with the desired properties.

Let $D = \max \deg(g)$. By multivariate Taylor expansion, we get for $j = 1, \dots, n$:

$$x^{(j)} = g^{(j)}(\lambda + h) = g^{(j)}(\lambda) + \sum_{i=1}^D \frac{1}{i!} \cdot \sum_{\substack{\alpha \in \mathbb{Z}_+^n : \\ \|\alpha\|_1 = i}} \frac{dg^{(j)}(\lambda)}{dx^\alpha} \cdot h^\alpha.$$

Therefore,

$$v_x^{(j)} = x^{(j)} - g^{(j)}(\lambda) = \sum_{i=1}^D \frac{1}{i!} \cdot \sum_{\substack{\alpha \in \mathbb{Z}_+^n : \\ \|\alpha\|_1 = i}} \frac{dg^{(j)}(\lambda)}{dx^\alpha} \cdot h^\alpha.$$

Note that $\max \deg \left(\frac{dg^{(j)}}{dx^\alpha} \right) < \max \deg(g)$ and that $0 \leq h < 1$ by construction.

This sum is a polynomial in λ and h , that is, it is a sum of terms $c_{\alpha,\beta} \lambda^\alpha h^\beta$. Since all $\lambda \geq 0$ we can use $0 \leq h_i < 1$, for all i , to bound the expression $c_{\alpha,\beta} \lambda^\alpha h^\beta$ by

$$0 \leq c_{\alpha,\beta} \lambda^\alpha h^\beta < c_{\alpha,\beta} \lambda^\alpha$$

if $c_{\alpha,\beta} > 0$ and by

$$c_{\alpha,\beta} \lambda^\alpha < c_{\alpha,\beta} \lambda^\alpha h^\beta \leq 0$$

if $c_{\alpha,\beta} < 0$. Putting now

$$g_l^{(j)}(\lambda) := \sum_{\alpha, \beta: c_{\alpha,\beta} < 0} c_{\alpha,\beta} \lambda^\alpha \quad \text{and} \quad g_u^{(j)}(\lambda) := \sum_{\alpha, \beta: c_{\alpha,\beta} > 0} c_{\alpha,\beta} \lambda^\alpha$$

we have

$$g_l^{(j)}(\lambda) \leq v_x^{(j)} \leq g_u^{(j)}(\lambda)$$

by construction. Moreover, again by construction, the degree of $g_l^{(j)}$ and of $g_u^{(j)}$ is strictly less than the degree of $g^{(j)}$. \square

The above theorem tells us that the error term v_x can be bounded by polynomials of strictly smaller maximal degree than that of $g(\lambda)$. As the following example shows, the degree of $g_l^{(j)}$ and of $g_u^{(j)}$ can in fact be much smaller than that of $g^{(j)}$.

Example 3.8 *Let us consider again the semi-algebraic set given by*

$$g(y) = \begin{pmatrix} y_1 \\ y_1^k + y_2 \end{pmatrix}.$$

As can be easily checked, each integral point v in this semi-algebraic set can be written as $v = g(\lambda)$ for $\lambda \in \mathbb{Z}_+^2$, showing that the correction term v_x is 0 in this case. \square

This leads us immediately to the questions of when is $v_x = 0$ or of when is $v_x \in \mathcal{C} \cap \mathbb{Z}^n$? In both cases, of course, $T = \{g(\lambda) : \lambda \in \mathbb{Z}_+^d\}$ would be an integral function basis for \mathcal{C} with our desired property $T \subseteq \mathcal{C} \cap \mathbb{Z}^n$.

We believe that research in this direction will make it possible to design novel algorithms for polynomial integer programming based on reformulation techniques.

References

- [1] D. Bertsimas and R. Weismantel. Optimization over Integers. Manuscript, 2004, Dynamic Ideas, Belmont Mass, to appear 2005.
- [2] F. R. Giles and W. R. Pulleyblank. Total dual integrality and integer polyhedra. *Linear Algebra and its Applications* 25 (1979), 191–196.
- [3] J. E. Graver. On the foundation of linear and integer programming I. *Mathematical Programming* 9 (1975), 207-226.
- [4] U. U. Haus, M. Köppe, and R. Weismantel. The integral basis method for integer programming. *Mathematical Methods of Operations Research*, 53 (2001).
- [5] Lenstra, H.W.: Integer Programming with a fixed number of variables. *Mathematics of Operations Research*, 8, (1983) 538–548.
- [6] A. Schrijver. *Theory of Linear and Integer Programming*. Wiley, Chichester, 1986.